

applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

4 Workshop on architectural support for security and anti-virus (WASSA): ChipLock:

support for secure microarchitectures

Taeho Kgil, Laura Falk, Trevor Mudge

March 2005 **ACM SIGARCH Computer Architecture News**, Volume 33 Issue 1

Publisher: ACM Press

Full text available:  pdf(256.52 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The increasing need for security has caused system designers to consider placing some security support directly at the hardware level. In fact, this is starting to emerge as an important consideration in processor design, because the performance overhead of supporting security in hardware is usually significantly lower than a complete software solution. In this paper, we investigate integrating some security support into hardware. We show that security support can be added at some acceptable cos ...

5 Mondrix: memory isolation for linux using mondriaan memory protection

Emmett Witchel, Junghwan Rhee, Krste Asanović

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available:  pdf(332.09 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

This paper presents the design and an evaluation of Mondrix, a version of the Linux kernel with Mondriaan Memory Protection (MMP). MMP is a combination of hardware and software that provides efficient fine-grained memory protection between multiple protection domains sharing a linear address space. Mondrix uses MMP to enforce isolation between kernel modules which helps detect bugs, limits their damage, and improves kernel robustness and maintainability. During development, MMP exposed two kerne ...

Keywords: fine-grained memory protection

Results 1 - 5 of 5

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4561	shared with librar\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:03
L2	202	I1 same task	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:04
L3	7	I2 same (key or cipher)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:06
L4	5	I3 and (processor or microprocessor)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:16
L5	19	I2 same (processor or microprocessor)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:29
L6	19	I1 with authenticat\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:38
L7	71	717/164.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L8	152	717/163.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L9	0	717/1623.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46

EAST Search History

L10	380	717/162.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:46
L11	54	I1 and (I7 or I8 or I9)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/20 10:47